Abschlussprüfung Winter 2023/24
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
1202

2 Analyse und Entwicklung von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=		100 – 92 Punkte	Note 2	=	unter	92 – 81 Punkte
Note 3	=	unter	81 – 67 Punkte	Note 4	=	unter	67 – 50 Punkte
Note 5	=	unter	50 – 30 Punkte	Note 6	=	unter	30 – 0 Punkte

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2023 – Alle Rechte vorbehalten!

1. Aufgabe (21 Punkte)

aa) 4 Punkte

Die Gateways zu den Netzen in Hamburg und München sind vertauscht, dies muss korrigiert werden. (Die Ziel-IP 10.1.1.2 muss beim Netzwerk 172.16.64.0 / 22 stehen und die Ziel-IP 10.2.2.0 muss beim Netzwerk 192.168.100.0 / 24 stehen.)

Sinngemäße Antworten sind auch richtig.

ab) 6 Punkte

Wegwahl wird durch das Routing-Protokoll bestimmt
Berücksichtigt im Vergleich zum statischen Routing den kürzesten, kostengünstigsten, schnellsten oder sichersten Weg
Überlastungen, Leitungs- und Knotenausfälle können durch Alternativ-Routen umgangen werden.
u. a.

ac) 4 Punkte

Für jeden Pfad durch das Netzwerk generiert jeder Routing-Algorithmus einen Wert, der als Metrik bezeichnet wird. Dabei ist ein Pfad umso besser, je geringer seine Metrik ist. Anhand dieses Werts sucht der Router die verwendete Route aus.

ad) 2 Punkte

- NAT/PAT (Destination-NAT)
- Portforwarding
- Getunnelte Verbindung mit VPN

Andere Lösungen sind möglich.

ba) 3 Punkte

WPA2/3 Enterprise stellt ein sicheres Authentifizierungsverfahren zur Verfügung und nutzt Protokolle und Standards wie das Extensible Authentication Protocol (EAP) und RADIUS.
Für die sichere Übertragung werden AES und CCMP als Verschlüsselungs- und Authentifizierungsmechanismus verwendet.

bb) 2 Punkte

Vorteile bei Enterprise:

- Für jeden Client lassen sich spezifische Anmeldedaten einrichten
- Logischer Zugang zu VLANs und WLANs möglich
- Ermöglicht unterschiedliche Zugriffsrechte im Netzwerk
- Einfache Sperre eines Accounts nach dem Austritt aus dem Unternehmen
- Logfiles für die Zugriffe der User können personalisiert erstellt werden

Andere Lösungen sind möglich.

2. Aufgabe (25 Punkte)

aa) 4 Punkte

NAT: Änderung der IP-Adresse auf dem Weg des Pakets
PAT: Änderung der Portnummer auf dem Weg des Pakets

ab) 3 Punkte

TTL: 128	Protokoll: 06	Header-Checksum: 54466
Quell-IP-Adresse: 172.16.32.150		
Ziel-IP-Adresse: 135.125.254.20		
Quell-Port: 49152		Ziel-Port: 443

ac) 5 Punkte

TTL: 126	Protokoll: 06	Header-Checksum: 32187
Quell-IP-Adresse: 203.0.113.13		
Ziel-IP-Adresse: 135.125.254.20		
Quell-Port: 50000		Ziel-Port: 443

ad) 2 Punkte
- Der Router wählt für ausgehende Verbindungen jeweils eine neue Quell-Port-Nummer, da intern auch Pakete mit identischer Quell-Port-Nummer bei ihm ankommen könnten.
- Über die Port-Nummern merkt er sich die Zuordnung, sodass er Antworten an den richtigen internen PC weiterleiten kann.

Andere Antworten sind möglich.

ba) 4 Punkte

Quell-IP-Adresse: 62.155.243.193	
Ziel-IP-Adresse: 203.0.113.13	
Quell-Port: beliebiger Wert zwischen 1024 und 65.535	Ziel-Port: 22

bb) 4 Punkte

Quell-IP-Adresse: 62.155.243.193	
Ziel-IP-Adresse: 10.10.10.2	
Quell-Port: beliebiger Wert zwischen 1024 und 65.535	Ziel-Port: 22

c) 3 Punkte
Der Provider versorgt die Kunden im Mobilfunknetz mit privaten IP-Adressen und übersetzt diese bei sich in öffentliche Adressen. Viele Kunden können mit einer einzigen, gemeinsamen IP das Internet nutzen. Nachteil Kunde: die Geräte beim Kunden sind nicht direkt aus dem Internet erreichbar, ggf. doppeltes NAT.

3. Aufgabe (28 Punkte)

a) 6 Punkte
- Bei Kupfer ist die **Reichweite** maximal 100 Meter. Abstand der Gebäude hier 150 Meter. Glasfaser hat eine größere Reichweite. (Multi-Mode ca. 500 bis 1.500 Meter; Single-Mode mehrere Kilometer)
- Höhere Bandbreite bei Glasfaser. Bei Kupferverbindungen sind Bandbreiten über eine Entfernung von 100 Metern nur mit aufwendiger Hardware möglich. Wenn die Bandbreite in Zukunft auf z. B. 40 Gbit/sec erweitert werden sollte, ist dies mit Kupfer nicht möglich. Eine **Glasfaserverbindung** ist bei der späteren Anforderung nach **höherer Bandbreite** zukunftssicherer.
- Glasfaserleitungen sind gegen **EMV-Störungen** unempfindlich. Wenn sich auf dem Leitungsweg größere elektrische Maschinen bzw. oder starke Magnetfelder befinden, wird die Signalübertragung nicht beeinflusst. Starke Magnetfelder können Kupferleitungen direkt beeinflussen bzw. die Signalübertragung stören.
- Glasfaserleitungen leiten keinen Strom. Bei zwei Gebäuden kann der Anschluss an das Stromnetz unterschiedlich erfolgen. Dadurch können die Gebäude auf unterschiedlichem Potenzial liegen. Bei einer Kupferleitung würde sich wegen des unterschiedlichen Potenzials ein Ausgleichsstrom (Brumm-Spannung) bilden. Dieser Strom würde das Signal beeinflussen. Da eine Glasfaserleitung keinen Strom leitet, sind die beiden Gebäude galvanisch getrennt. Eine sogenannte Brumm-Spannung ist durch diese **„Galvanische Trennung"** nicht möglich.
- Glasfaser bietet einen **Schutz vor Überspannung (Blitzschlag)**. Bei einem Blitzeinschlag in einem der beiden Gebäude oder in den Leitungsweg wird die Energie nicht weitergeleitet. Eine Kupferleitung würde die Energie des Blitzschlages auf alle angeschlossenen Geräte weiterleiten und diese in Mitleidenschaft ziehen.

Weitere Lösungen sind möglich.

ba) 4 Punkte
Mehr Sicherheit, da logische Trennung der Netzwerksegmente
Mehr Flexibilität, da neue Netzsegmente leicht erzeugt werden können
Weniger Hardware, da mehrere Netzwerksegmente auf einem Switch/Kabel laufen
Weniger Kosten, da weniger Hardware angeschafft werden muss
Weniger Verkabelung, da mehrere Netzwerksegmente auf einem Switch/Kabel laufen

Andere Lösungen sind möglich.

bb) 2 Punkte
(V)LAN-Verbindungen zwischen den Switches müssen an den UpLink-Ports auf „tagged" eingestellt werden.

Ähnliche Lösungen (herstellerabhängig) sind möglich.

bc) 3 Punkte
Im OSI-Layer 2 wird ein VLAN-Tag eingefügt. (Dies beinhaltet die Kennzeichnung für VLAN und die VLAN-Nummer.)

Ähnliche Lösungen sind möglich.

ca) 3 Punkte
- Keine Antwort vom eingetragenen DNS (192.168.100.1) erhalten
- DNS-Serverdienst (192.168.100.1) ist nicht erreichbar

cb) 2 Punkte
192.168.100.212

cc) 2 Punkte
VLAN 11

cd) 6 Punkte
Fehlerursache:
Client und Router sind in verschiedenen VLANs konfiguriert. Ein Routing zwischen diesen VLANs findet nicht statt.

Andere Lösungen sind möglich.

Fehlerbeseitigung:
- Den Switch-Port des Clients in das gleiche VLAN wie den Internetrouter aufnehmen.
- Ein Routing zwischen den VLAN 11 und den VLAN des Internetrouters konfigurieren.

Weitere Lösungen sind möglich.

4. Aufgabe (26 Punkte)

a) 4 Punkte
- Kann nicht so leicht ausspioniert werden
- Angriffe über Social-Engineering nicht möglich
- Kann an Geräte bzw. Mitarbeiter gebunden werden
- Höhere kryptografische Sicherheit (Schlüssellängen)

Weitere Antworten sind möglich.

ba) 4 Punkte
Beim Signieren eines Zertifikates durch eine CA wird nicht das gesamte Zertifikat signiert (mit dem Private Key der CA verschlüsselt). Es wird lediglich ein Hashwert des Zertifikates gebildet und signiert, der (bei Kollisionsfreiheit) das Zertifikat eindeutig identifiziert.

bb) 4 Punkte
Bei einem Kollisionsangriff (collision attack) ist es möglich, ein gefälschtes Zertifikat zu erzeugen, welches den gleichen Hashwert hat wie das ursprüngliche. Dadurch werden gefälschte Zertifikate nicht als solche erkannt, sondern akzeptiert. MD5 ist anfällig für Kollisionsangriffe.

ca) 4 Punkte
Der private Schlüssel der CA ist an die Mail angehängt worden. Damit ist er nicht mehr privat (geheim), und die gesamte CA ist kompromittiert.

cb) 4 Punkte
Die gesamte CA muss neu angelegt werden bzw. alle Schlüssel der CA müssen neu generiert werden.
Anschließend müssen sämtliche Zertifikate, die von der alten CA signiert wurden, durch neue ersetzt werden.

(Hinweis: sollte nur der erste Schritt genannt werden, gibt es 2 Punkte. Die 2 weiteren Punkte nur, wenn erkannt wurde, dass alle Client-Zertifikate ausgetauscht werden müssen.)

da) 3 Punkte
DH ist ein Verfahren zum Generieren von symmetrischen Schlüsseln über einen offenen Kanal. Es wird von TLS1.3 genutzt, um auf beiden Seiten einen symmetrischen Session-Key zu erzeugen.

db) 3 Punkte
Asymmetrische Verschlüsselung wird bei TLS1.3 ausschließlich zur Authentifizierung bzw. zum Überprüfen der Signaturen der Zertifikate eingesetzt.